ABSTRACT OF THE DISCLOSURE

A method and apparatus for performing ephemeral communication and assuring that an ephemeral decryption key is not accessible subsequent to an expiration time associated with the respective key. An ephemeral key pair is preferably generated within a tamper resistant cryptographic processor unit. The ephemeral key pair comprises and ephemeral encryption key and an ephemeral decryption key. The ephemeral decryption key is prevented from being accessed external of the tamper resistant cryptographic processor unit. Ephemeral messages encrypted using an ephemeral encryption key are decrypted by the cryptographic processor unit if associated with a time that precedes the expiration time for the respective ephemeral decryption key. A decrypted ephemeral message is prevented from being transmitted from the cryptographic processor unit in the event a time associated with a received encrypted ephemeral message is subsequent to the expiration time for the respective ephemeral key pair.

241084

ATTORNEY DOCKET NO. P5529
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES LLP
TEL. (617) 542-2290
FAX. (617) 451-0313